CYBER SECURITY 2010

22 - 23 September, 2010, Hotel La Plaza, Brussels, Belgium

Contingency Planning

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

© Peter Sommer, 2010

LSE

Assumptions

- Your detective and preventative measures have failed - the cyber event has started and you need to mitigate and recover
- Why?
  - ➔ Zero day exploits
  - ➔ Your system is being overloaded because of problems elsewhere
  - ➔ You are under attack, but can't retaliate because you lack sufficient attribution of the source

A Contingency Plan may be your best defence against Cyber Attack

LSE

Experience of Contingency Planning

- **Knowledge and experience exists in the commercial sector**
  - ➔ **Sub-industry of specialist stand-by facilities**
  - ➔ **Skills in detailed planning and testing**
- **Some Governments have significant Civil Contingencies experience**
  - ➔ **Bombs, Floods, Escape of Noxious substances, Pandemics, Industrial Unrest, Earthquakes, etc**
- **How far does this extend to the Cyber Domain?**

© Peter Sommer, 2010

LSE

Basics of Disaster Recovery

The chances of being hit have almost nothing to do with the chances of successful recovery

You need to understand what recovery looks like – and how it takes place

© Peter Sommer, 2010

LSE

Disaster Recovery

The chances of being hit:

- Logical / Cyber attack
- Bomb, kinetic attack
- Fire
- Flood
- Electrical outage
- Computer failure – hardware, software
- Telecoms failure

➢ Preventative / Detective Measures

© Peter Sommer, 2010

LSE

Disaster Recovery

The chances of successful recovery (commercial businesses):

- **Cash flow / overheads / indebtedness**
- **Business organisation**
- **Perishability of products / services**
- **Single site / multiple site**
- **Computer dependency**

➢ **Recovery and Mitigation Plan**

© Peter Sommer, 2010

LSE

Disaster Recovery

The chances of successful recovery (central government service):

- **Single site / multiple site**
- **Possibility of transfer of operations**
- **Computer dependency**
- **Internal organisation – especially speed of response**
- **Status of any outsourcing contract**
- **Quality of political leadership**
- ➢ **Recovery and Mitigation Plan**

© Peter Sommer, 2010

LSE

Business Continuity Planning

Most BCP is carried out in two stages:

- **vulnerability assessment**
  - ➔ **part of risk management process**
- **recovery plan**
  - ➔ **deciding what you actually will have to do**

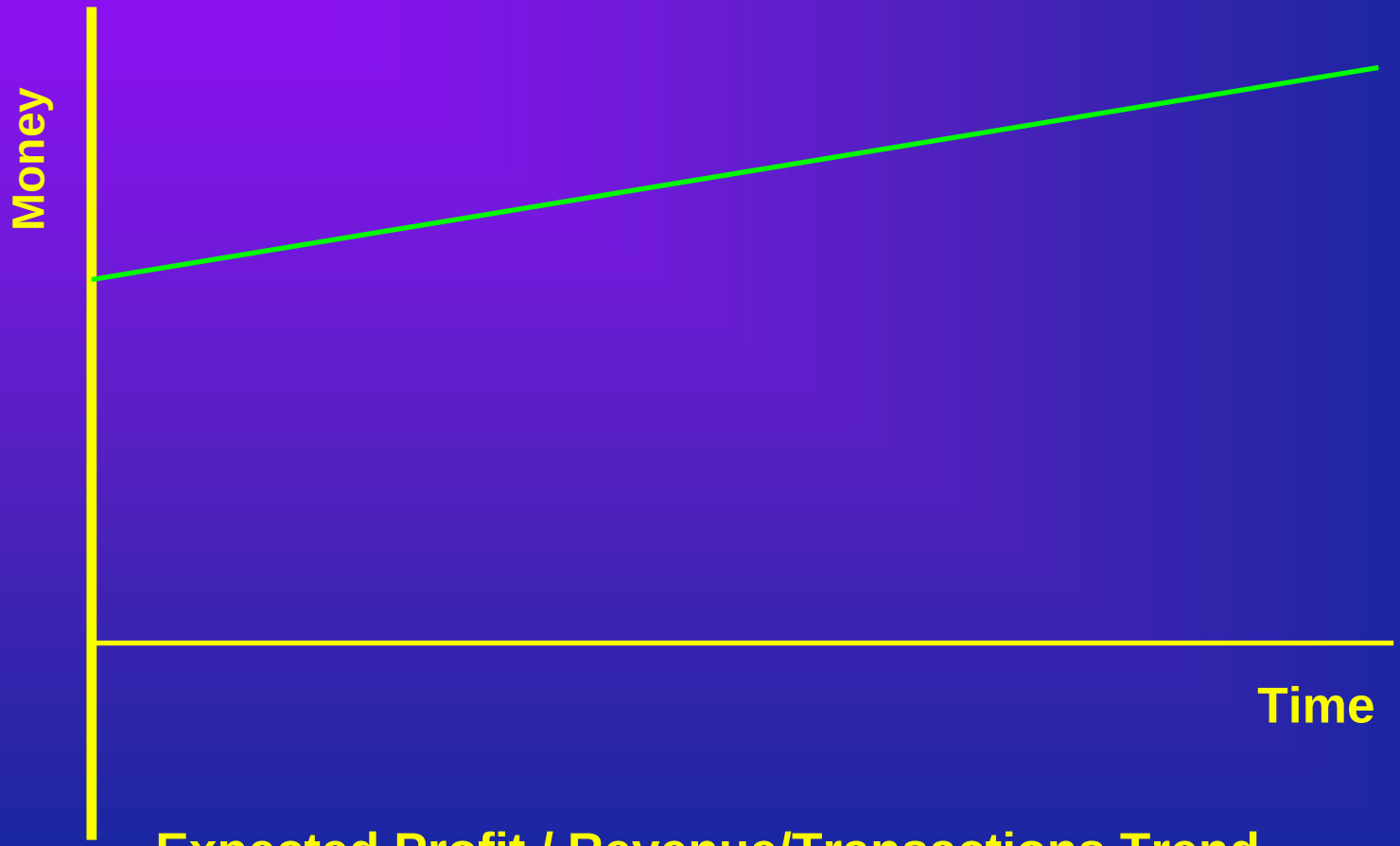
© Peter Sommer, 2010

LSE

Shape of Disaster

© Peter Sommer, 2010

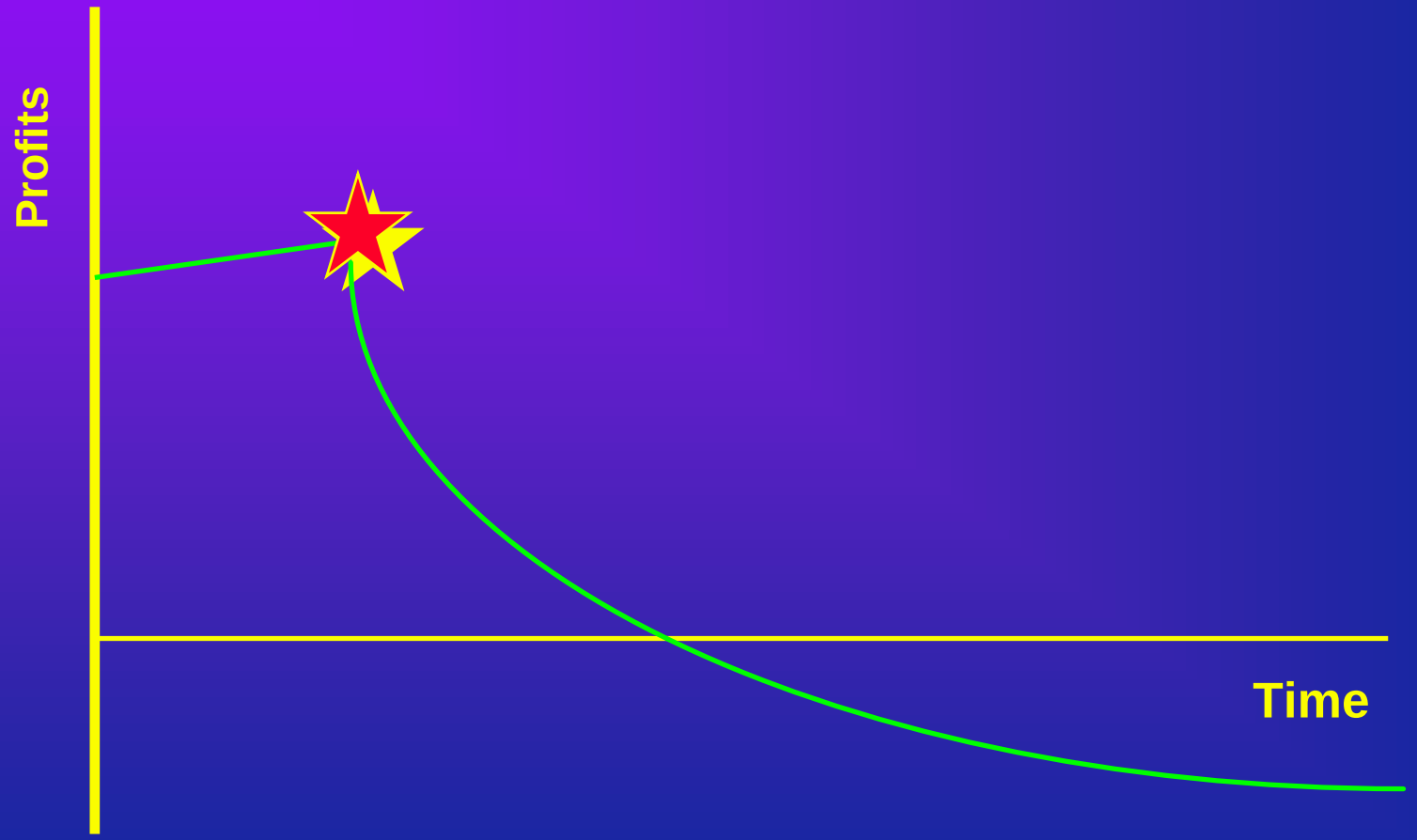
Shape of Disaster



Expected Profit / Revenue/Transactions Trend

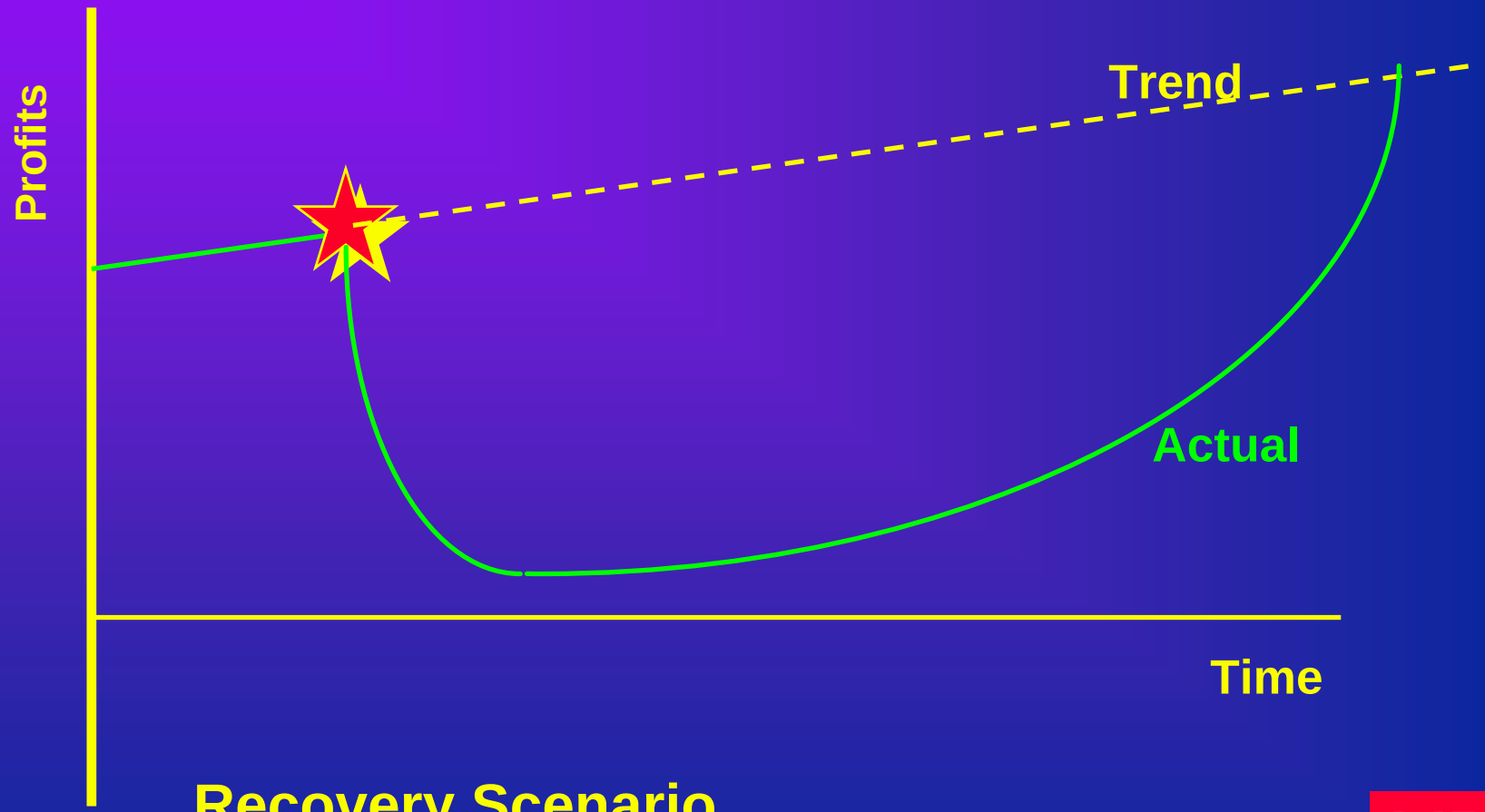
© Peter Sommer, 2010

Shape of Disaster



© Peter Sommer, 2010

Shape of Disaster

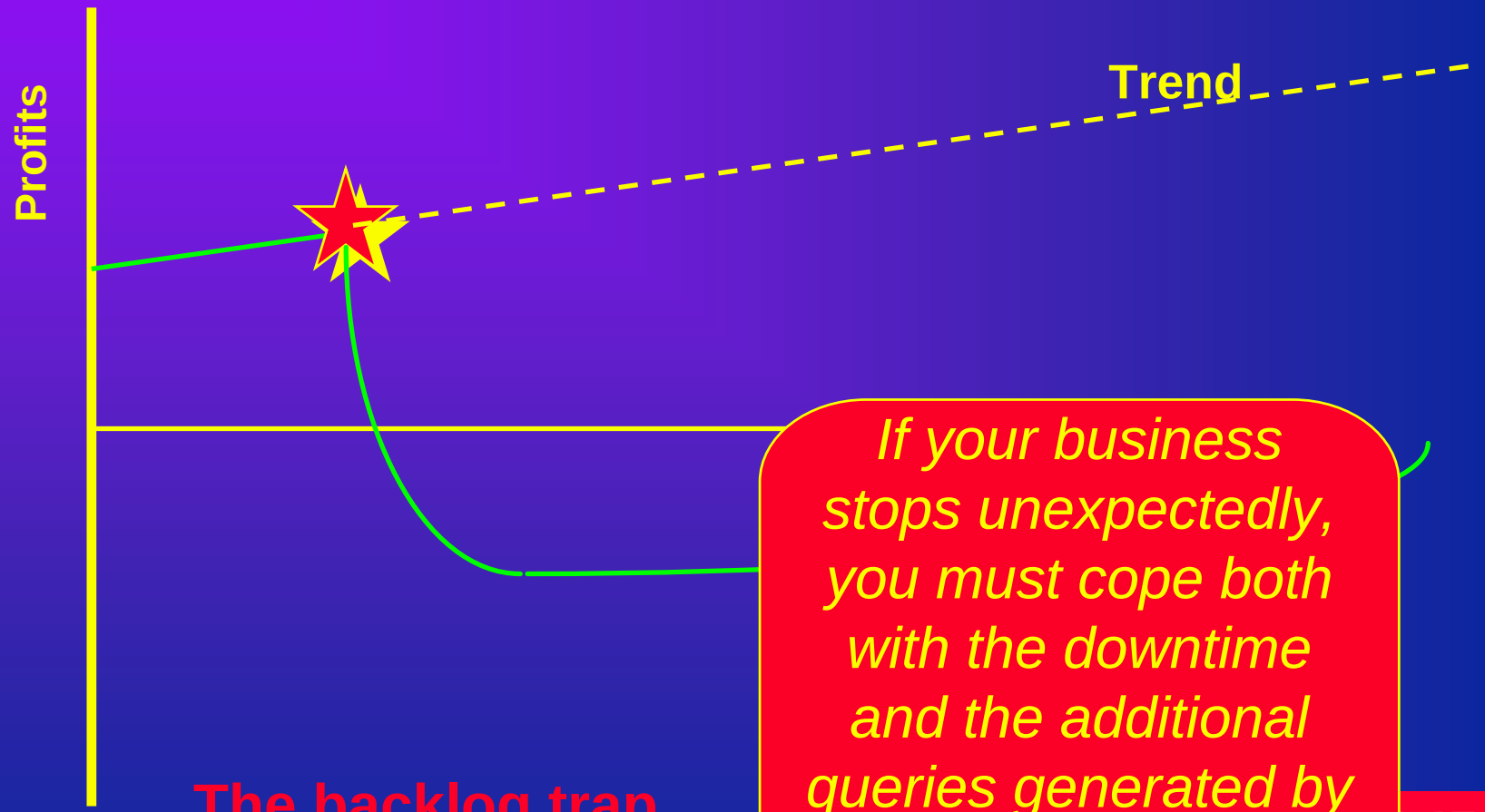


Recovery Scenario

© Peter Sommer, 2010

LSE

Shape of Disaster



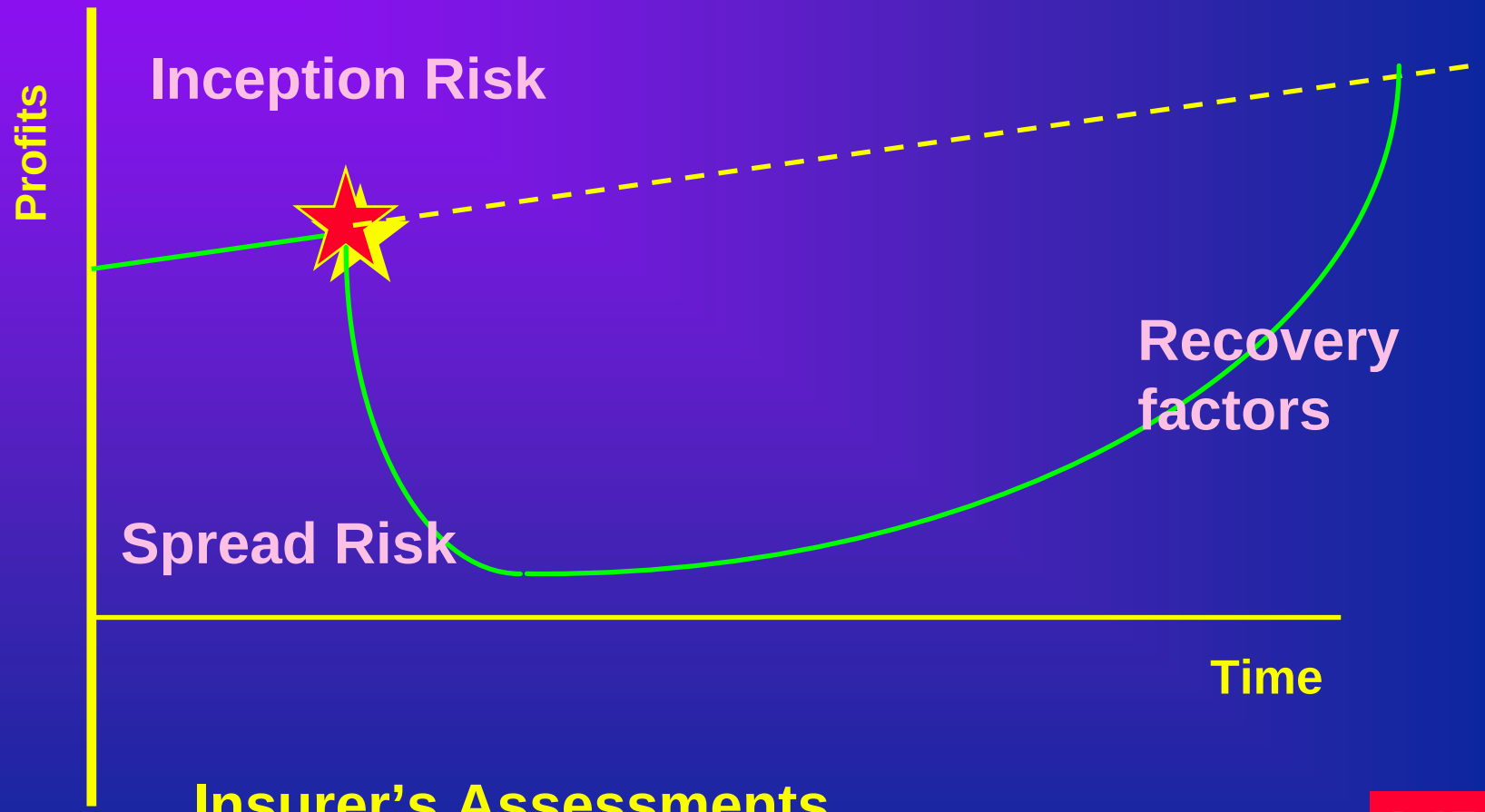
If your business stops unexpectedly, you must cope both with the downtime and the additional queries generated by the downtime

The backlog trap ……

© Peter Sommer, 2010

LSE

Shape of Disaster

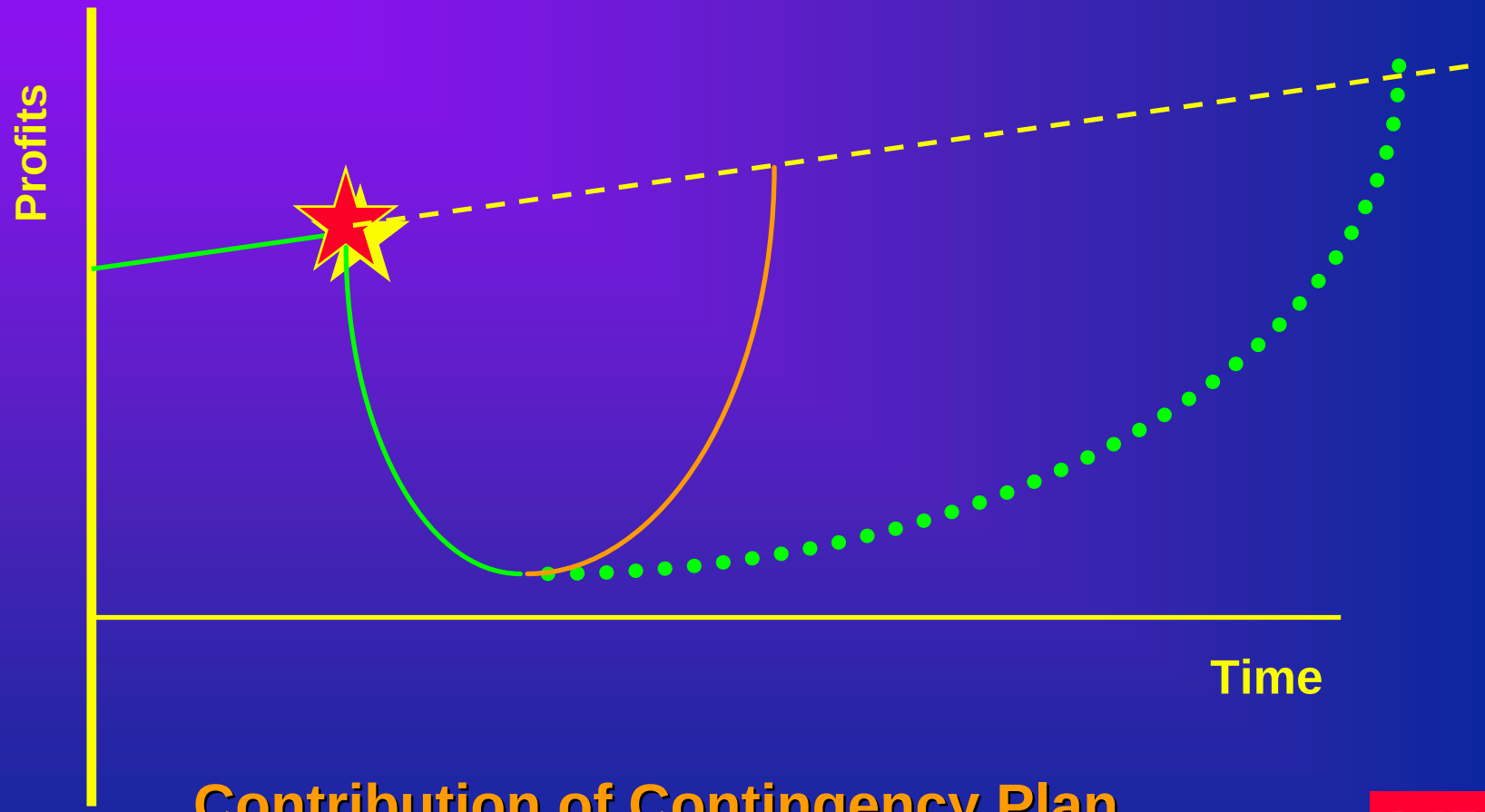


Insurer's Assessments..

© Peter Sommer, 2010

LSE

Shape of Disaster



Contribution of Contingency Plan..

© Peter Sommer, 2010

LSE

What You Need to Know

- **Spread Risk**
  - → How might an initial event propagate and cascade?
- **Recovery Factors?**
  - → What is already available?
  - → What do you need to acquire / prepare for?

© Peter Sommer, 2010

LSE

Spread Risk

- Propagation and Cascade
- Historically cyber-events have not lasted very long:
  - ➔ Signatures of attacks, responses to zero-day vulnerabilities often found within a few days
  - ➔ The longer a botnet exists, the greater the chance the controller will be identified
- But each potential threat needs to be tested out for local circumstances

© Peter Sommer, 2010

LSE

Spread Risk: Propagation and Cascade

At the level of the nation state, you also need to think about:

- Impact on CII services
- Impact on very vulnerable people
- Impact on efficiency of emergency services
- Impact on politics / public confidence
- Acceptable levels of failure

© Peter Sommer, 2010

LSE

Recovery Factors

- You can't bring back a 100% service immediately – so what should you prioritise?
- What is already available that can be deployed?
  - ➔ Back-up data
- What do you need to acquire / prepare for?
  - ➔ Management structure
  - ➔ A Plan
  - ➔ Recovery Sites
  - ➔ Third Party facilities

© Peter Sommer, 2010

LSE

Business Continuity Planning

In order to save an organisation from extinction after a disaster...

- **We need to know how it operates**
  - ➔ **what are its essential functions?**
    - **operational**
    - **managerial**
  - ➔ **(commercial) where does its income come from?**
  - ➔ **(state) potential for social unrest**

© Peter Sommer, 2010

LSE

Business Continuity Planning

This is essentially a business and/or social science type analysis

- **(Commercial): immediate revenue generation and confidence building with customers, trading partners, staff, bankers, etc usually a priority over R&D and marketing**
- **(Nation State) Impact on very vulnerable people; impact on efficiency of emergency services; impact on politics / public confidence**

© Peter Sommer, 2010

LSE

Business Continuity Planning

- **We need a plan:**
  - → to identify priorities based on business need
  - → a dedicated team, distinct from the main management team
  - → detailed recovery procedures against likely disaster scenarios

Companies recover from disasters in complex, unexpected ways ...

© Peter Sommer, 2010

LSE

Business Continuity Planning

The chances of successful recovery:

- **the backlog trap**
- ***the return to normal from a "system down" takes 5 x the downtime period - if you are able to increase the effective wor immediately***

During recovery you must both recover and carry on normal activity – and deal with enquiries about "lost" work

©Peter Cornell, 2010

LSE

Business Continuity Planning

(Commercial) The chances of successful recovery:

- **the longer recovery takes the greater the chance of failure because of:**
  - ➔ **loss of staff motivation**
  - ➔ **customer defection**
  - ➔ **pressures on credit position**
    - **difficulty in getting credit from suppliers**
    - **difficulty in collecting debts**
    - **loss of bank confidence**

© Peter Sommer, 2010

LSE

Business Continuity Planning

(National State) The chances of successful recovery:

- **the longer recovery takes the greater the chance of failure because of:**
  - → **Loss of public confidence**
  - → **Leading to social unrest**

© Peter Sommer, 2010

LSE

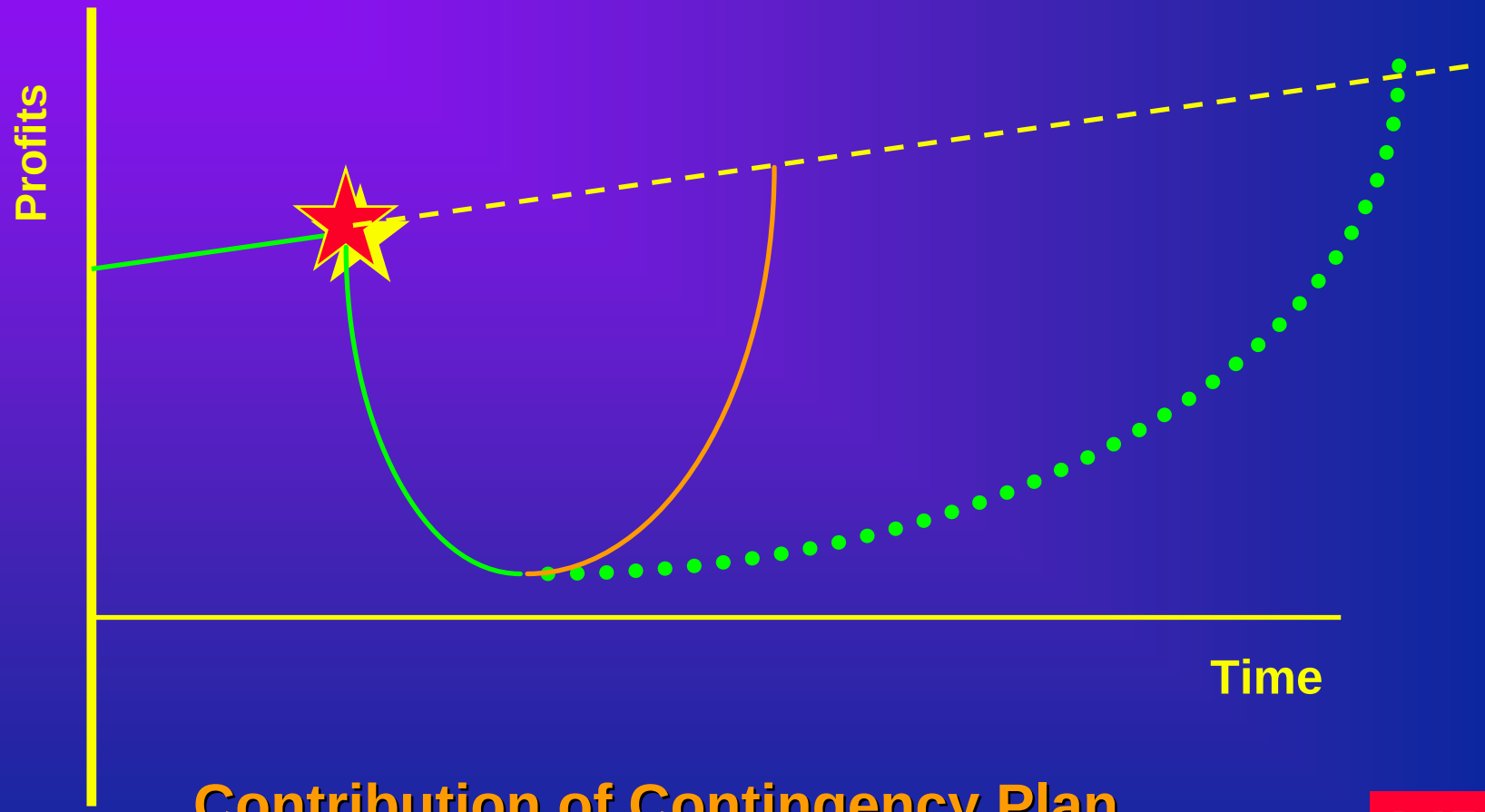
Business Continuity Planning

- Total instant recovery implies a fully duplicated set of computer and network resources – plus instant mirroring
- Most people settle for less than that – you have to decide how much less is "acceptable"
- You can give different priorities to different parts of your organisation

© Peter Sommer, 2010

LSE

Shape of Disaster



Contribution of Contingency Plan..

© Peter Sommer, 2010

LSE

Shape of Recovery

Levels of Functionality by time

Within 2 hrs	10%
Within 24 hrs	25%
Within 7 days	50%
Within 3 months	90%

What you can achieve is a function of how much you spend, how wisely you spend, and the quality of your plan

© Peter Sommer, 2010

LSE

Managing the Recovery

- Dedicated team reporting to top management (top management need to concentrate on welfare of organisation as a whole, not the detail of recovery)
- IT, telecoms
- buildings facilities
- human resources
- legal
- press liaison

© Peter Sommer, 2010

Business Continuity Planning

Detailed recovery procedures against likely disaster scenarios

- **buildings**
- **equipment**
  - → **office**
  - → **computers**
  - → **telecoms**
  - → **machinery**
- **people**

© Peter Sommer, 2010

LSE

Disaster Recovery Facilities: what the market can offer

- Computer Resources
- Network Resources
- Resilient Web-servers
- (consultancy)

© Peter Sommer, 2010

Computer Disaster Facilities

- **Instant Restart**
  - ➔ Fully duplicated systems – very high costs
- **Hot restart**
  - ➔ (A few hours): Stand-by systems, updated configuration information plus up-to-date back-up, plus technical support
- **Warm restart**
  - ➔ (24-48 hours) Stand-by systems, may require specific configuration information plus up-to-date back-up
- **Cold restart**
  - ➔ (48 + hours) Stand-by system of agreed specification, but no pre-configuration; users responsible for the rest

© Peter Sommer, 2010

LSE

Computer Disaster Facilities

- **Hot restart**
- **Warm restart**
- **Cold restart**

These are based on the nation of facilities shared between a number of clients and in the hope that only one at a time will need them:

- ***Ratio of facilities to potential users***
- ***How does this fit in with your disaster scenario?***

If your system is very large or unusual you may not be able to get commercial standby facilities

© Peter Sommer, 2010

LSE

Network Recovery Facilities

- Dual Source / Routing supply
- Your own infrastructure facilities: switches, modems, telecommunications hubs etc: you need to have documents for potential emergency configurations – plans to operate from alternate premises
- Unless the network supplier is also hit by a catastrophe, purchasing additional capacity should be relatively easy
- If you are a very large customer you may need to make enquiries about “upstream” facilities

© Peter Sommer, 2010

LSE

Resilient Web-Servers

- **Problems:**
  - Likely attack is via DDoS / Botnets or poisoned addressing/routeing
  - If you change the IP address of uyour web-server, customers will not be able to find it. (Or when they do, so will the attackers)
- **Solutions:**
  - distributed computing platform for global Internet content and application delivery
  - Large system load-balancing

© Peter Sommer, 2010

LSE

Particular Problems for Nation States

- **Reliance on Out-sourcing**
  - → Failure of Government Service
  - → Overload of Government Information facility during a disaster
  - → What does contract say? What compensation for loss of service?
  - → If out-sourcer fails, can government tale over?
    - Contractual issues
    - Operational Practicalities

© Peter Sommer, 2010

LSE

Particular Problems for Nation States

- How to manage?
- Legal bases / authority
- Is this a job for the military or civilian parts of government?
- How, and how far, is political control exercised?
  - ➔ Political, democratic accountability
- How is this to be funded?

© Peter Sommer, 2010

LSE

Particular Problems for Nation States

- **Public Private Partnerships**
  - ➔ Much of the CII / CNI is in private ownership but provides services the public rely on
  - ➔ How far can a Government require a CII/CNI business to plan to serve a broad public safety agenda – as opposed to protecting revenue/profit?
  - ➔ Who pays for any additional costs involved?

© Peter Sommer, 2010

LSE

International Contingency Plans

- Most “international” work relates to law enforcement – CoE Cybercrime Treaty
- Almost nothing is being done on international contingency plans – any required action would be completely ad hoc
  - ➔ Many countries have yet to determine their own cybersecurity and cyber contingency plan strategies

© Peter Sommer, 2010

LSE

Finally

- Contingency Plans are essential because
  - ➔ some attacks will succeed
  - ➔ You will not know who is attacking and you cannot therefore deter by threat of retaliation
- The chances of successful recovery have no connection with your vulnerability to being hit
- You need to understand the spread risk – the extent to which an initial event may propagate
- You need to prioritise what you want to recover and at what speed
- You need a great deal of pre-planning
- You need a separate team to execute the plan

© Peter Sommer 2014

LSE

22 - 23 September, 2010, Hotel La Plaza, Brussels, Belgium

Contingency Planning

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

© Peter Sommer, 2010

LSE